Vulnerability Disclosure Policy
City of Longmont
11/2019

Introduction

The City of Longmont is committed to ensuring the security of the American public by protecting their information from unwarranted disclosure. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy describes **what systems and types of research** are covered under this policy, **how to send us** vulnerability reports, and **how long** we ask security researchers to wait before publicly disclosing vulnerabilities.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered – as set out in this policy – so we can fix them and keep our users safe. We have developed this policy to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith.

Guidelines

We request that you:
- Notify us as soon as possible after you discover a real or potential security issue.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to "pivot" to other systems.
- Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test, notify us immediately, and not disclose this data to anyone else**.
- Do not submit a high volume of low-quality reports.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized, we will work with you to understand and resolve the issue quickly, and the City of Longmont will not recommend or pursue legal action related to your research.

Scope

This policy applies to the following systems and services:

- *.longmontcolorado.gov

Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in non-City systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system or endpoint is in scope or not, contact us at security@longmontcolorado.gov before starting your research.

Though we develop and maintain other internet-accessible systems or services, we ask that *active research and testing* only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that you think merits testing, please contact us to discuss it first. We will increase the scope of this policy over time.

The following test types are not authorized:

- Network denial of service (DoS or DDoS) tests
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

Reporting a vulnerability

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities.

We accept vulnerability reports via security@longmontcolorado.gov. Reports may be submitted anonymously.

We will acknowledge receipt of your report within 5 business days.

We do not support PGP-encrypted emails at this time.

What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports:

- Describe the vulnerability, where it was discovered, and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Be in English, if possible.

What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within 5 business days, we will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.